Plackovací práce 2022

Táborové šifry

TK Modrý Kruh – oddíl ROJ

Alexandr Sekera
Pavián

Obsah

Úvod

Šifry jsou potřeba už odjakživa. Občas mezi sebou potřebujeme komunikovat tak, aby nám ostatní nerozuměli. Na našem táboře se šifry používají především na takzvaných „puťácích“, kdy děti chodí po zaluštěných zprávách, které je odkazují na další. Puťáky samozřejmě nejsou jedinou aktivitou, kdy se u nás šifry používají. Jejich znalost je nutná při různých hrách na táboře a při plnění úkolů v celoroční činnosti. Šifrování je zajímavou formou zábavy, kdy člověka dokáže uspokojit, že ji zvládl vyřešit. Zároveň nám šifry dokážou rozvinout programovací myšlení, které nemusí být nutně využito pouze k programování, ale například i ve škole.

V práci se věnuji táborovým šifrám oddílu ROJ. Pokusím se vysvětlit podstatu šifry a uvést podrobný návod, jak text do určité šifry zaluštit a jak ho i vyluštit. Ještě existují šifry logické, které zde ale obsažené nejsou.

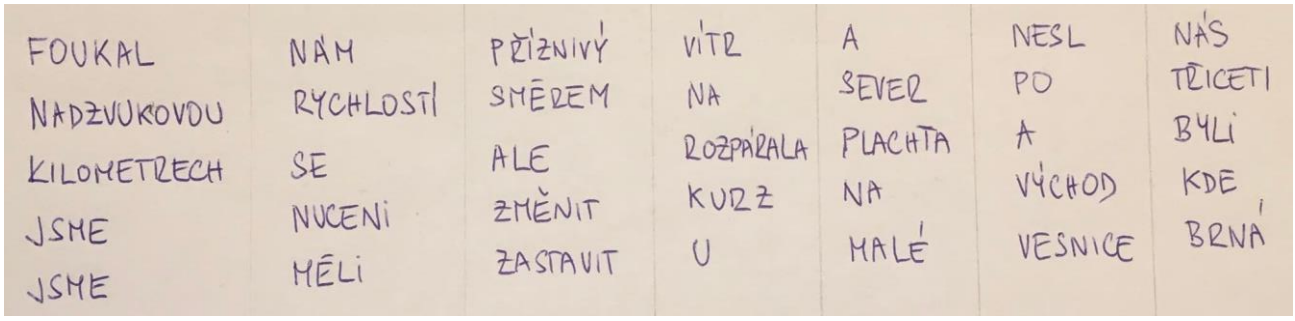
Lístečková šifra

První táborovou šifrou je lístečková. Tato šifra je jednoduchá a její příprava je taktéž velmi jednoduchá.

Zaluštění

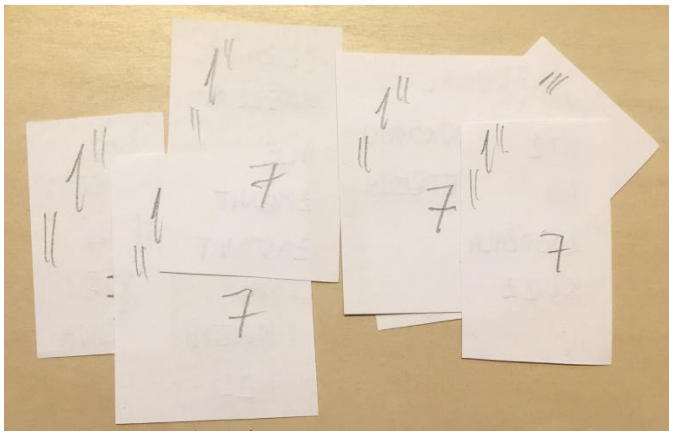
Ukážeme si šifru na praktickém příkladu. Vezmeme si větu „***Foukal nám příznivý vítr a nesl nás nadzvukovou rychlostí směrem na sever. Po třiceti kilometrech se ale rozpárala plachta a byli jsme nuceni změnit kurz na východ, kde jsme měli zastavit u malé vesnice Brná.***“. Nejprve si spočítáme počet slov. Těch je momentálně 35. Nyní se musíme rozmyslet, jak slova rozřadíme na lístečky. 35 se dá rozložit na součin 5 × 7, což nám dává krásnou možnost pěti slov po sedmi lístečkách. Rozdělíme si tedy papír na sedm sloupců a začneme slova postupně vpisovat.

Následně se lístečky nastříhají a označí příslušnými znaky. Náročnost šifry se odlišuje podle věku a zkušenosti dětí. Například vzorovou větu bych doporučil dětem, které už někdy nějakou šifru vyluštily, ale nejstarším dětem bych náročnost zvýšil. Pokud nám nevyhovují násobky, věta se dá vždy přeformulovat tak, aby byla delší nebo kratší. Také si můžeme pomoct označováním interpunkce jako slov, tzn. psát interpunkci do sloupců na řádky jako všechna ostatní slova. Musíme se vždy nějak přizpůsobit, nic není nemožné.



Obrázek 1: Náčrt lístečkové šifry

Označuje se číslicí 1 na každém lístečku společně s počtem lístečků pro případ, že by se některý z nich ztratil. V takovém případě řešitel ví, že se šifra nyní nedá vyluštit a musí situaci vyřešit jiným způsobem.



Obrázek 2: Hotová lístečková šifra

Vyluštění

U lístečkové šifry nejde o nic těžkého. Jednoduše se snažíme lístečky poskládat tak, aby nám ze slov vycházel smysluplný text. Občas nám autor šifry napoví, když používá malá a velká písmena. Pak totiž

dokážeme odhadnout, kde začíná a kde končí věta. Pokud je na některých lístečcích méně slov než na ostatních, logicky víme, že musí být jako poslední lístečky. Občas jsme díky tomuto schopni hned na začátku odhalit poslední lísteček.

Řádková šifra

Druhou táborovou šifrou je řádková. Řádková šifra je mezi dětmi obecně neoblíbená, protože není hned očividné, jakou kombinaci klíče použít k jejímu vyluštění. Na druhou stranu děti cítí úžasný pocit, když se jim konečně podaří klíč a správný násobek odhalit. Dle mého názoru se ale jedná o velmi hravou a zábavnou šifru.

Zaluštění

Nejprve si musíme spočítat počet znaků, které máme ve větě. Pokud nám opět nebudou vycházet dobré násobky (například prvočísla), musíme se přizpůsobit. V tomto případě opět můžeme počítat s interpunkcí a jakoukoliv úpravou textu jako se samostatným znakem, ale před tímto krokem je lepší nejdřív vymyslet znění věty jinak. U řádkové šifry můžeme také ale využít i výplňová písmena nebo slova. Slovem musí být něco, co je nezmate a nesplete, takže mluvíme o nějakém „prázdném“ slově. U znaků je to daleko jednodušší, protože se používá písmeno ‚X‘ (také křížek).

Použijeme větu z minulého oddílu. Věta má 174 znaků včetně interpunkce, což je krásný násobek čísla 6, protože 174 = 6 × 29. V této ukázce ovšem místo interpunkce vložím dva křížky. Následně si nakreslíme obdélník, do kterého budeme text vpisovat.

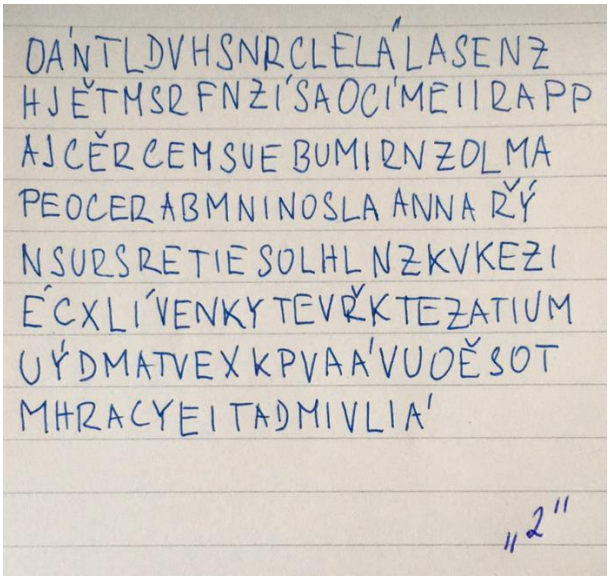
2	O	Á	N	T	L	D	V	H	S	N	R	C	L	E	L	Á	L	A	S	E	N	Z	H	J	Ě	T	M	S	R
1	F	N	Z	Í	S	A	O	C	Í	M	E	I	I	R	A	P	P	A	J	C	Ě	R	C	E	M	S	U	E	B
3	U	M	I	R	N	Z	O	L	M	A	P	E	O	C	E	R	A	B	M	N	I	N	O	S	L	A	A	N	N
5	A	Ř	Ý	N	S	U	R	S	R	E	T	I	E	S	O	L	H	L	N	Z	K	V	K	E	Z	I	É	C	X
6	L	Í	V	E	N	K	Y	T	E	V	Ř	K	T	E	Z	A	T	I	U	M	U	Ý	D	M	A	T	V	E	X
4	K	P	V	A	Á	V	U	O	Ě	S	O	T	M	H	R	A	C	Y	E	I	T	A	D	M	I	V	L	I	Á

Tabulka 1: Připravená řádková šifra

Tabulka je rozdělená na 6 řádků a 29 sloupců, každý čtvereček reprezentuje náš znak. Nyní si musíme zvolit klíč, kterým šifru zaluštíme. Na obrázku je zvolen klíč ‚213564‘, podle kterého budeme vpisovat nezaluštěný text do příslušných políček.

Na konci nám nezbývá nic jiného, než text přepsat a zkontrolovat. Správně by se měly kontrolovat všechny šifry, ale některé se musí kontrolovat více. Konkrétně u řádkové šifry je velmi snadné se splést.

Označuje se číslicí 2 na kusu papíru, kde je napsaná i celá šifra. Další znaky nejsou potřeba vzhledem k povaze šifry.



Obrázek 3: Hotová řádková šifra

Vyluštění

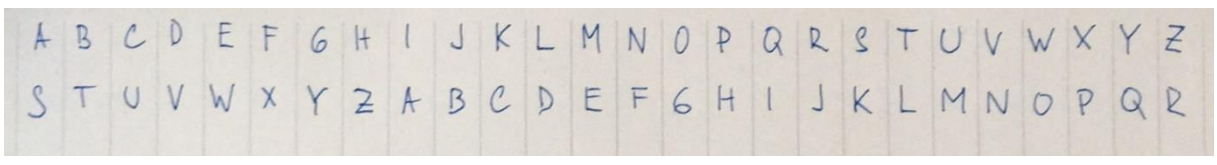
Nejprve si musíme spočítat znaky. Po napočítání 174 znaků si vymyslíme, jaké násobky můžeme použít. Správnou odpovědí je 6 × 29, ale také nás může napadnout 2 × 87 a 3 × 58. Samozřejmě nesmíme opominout i obrácené násobky, tj. 29 × 6, 87 × 2 a 58 × 3. Z těchto šesti násobků ovšem dává smysl jen jeden, a to náš správný. Často není násobek tak očividný, občas musíme projet až několik tabulek, než najdeme tu správnou. Ve chvíli, kdy najdeme správnou tabulku, musíme odhadnout správnou číselnou kombinaci.

Posunka

Třetí táborovou šifrou je takzvaná „posunka“. Ve skutečnosti se jedná o obyčejnou Caesarovu šifru, ale pro náš kruh nám přišel název posunka výstižnější a jednodušší na zapamatování pro všechny děti. Jedná se o šifru vcelku jednoduchou, ale pořád dokáže zamotat hlavu, hlavně během zalušťování.

Zaluštění

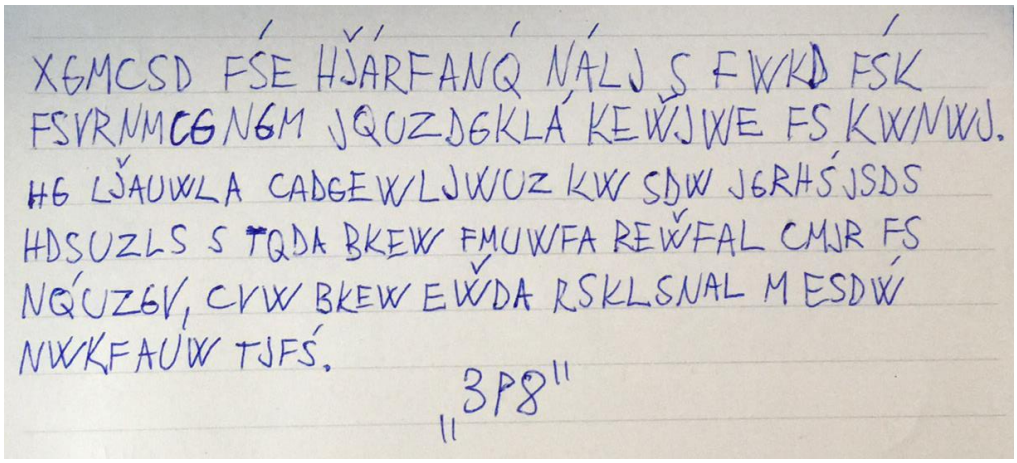
Opět použijeme větu z prvního oddílu. Následně si napíšeme anglickou abecedu, která se skládá z 26 písmen. Po napsání se musíme rozmyslet, na jakou stranu a o kolik písmen budeme abecedu posouvat. Vzorově si zvolíme pravou stranu a 8 znaků. Napíšeme si tedy novou abecedu, ovšem posunutou doprava o osm znaků.



Obrázek 4: Příprava posunky

Nyní musíme text zaluštit. Musíme si pamatovat, v jaké abecedě se zrovna pohybujeme, protože když si uprostřed luštění uvědomíme, že pracujeme opačně, musíme začít od znova. Zalušťuje se seshora dolu. V našem případě by se ze slova BRNÁ stalo TJFŚ, diakritika může zůstat. Občas to dokáže napovědět, protože písmeno ‚F‘ s kroužkem v naší abecedě nenajdete a jen jedno písmeno u nás má kroužek. Po přepisu se opět vrhneme na kontrolu.

Označuje se číslicí 3, která je obohacena o příslušné písmenko P (posunuto vpravo) nebo L (posunuto vlevo) a další číslicí, která určuje počet písmen, o kolik se abeceda posouvá. V tomto případě bychom napsali „3P8“.



Obrázek 5: Hotová posunka

Vyluštění

Nejprve si musíme napsat anglickou abecedu. Následně využijeme strany a čísla napsané u označení šifry. Odpočítáme si počet znaků do příslušné strany a začneme rozepisovat opět abecedu. Po napsání obou abeced si přečteme zaluštěný text a každý znak jednotlivě vyluštíme. Vkládáme znaky odspoda nahoru, dokud nám nevyjde původní text.

Mřížka

Čtvrtou táborovou šifrou je mřížka. Šifra jednoduchá na vyluštění, ale velmi náročná na zaluštění. Jedná se o celkem oblíbenou šifru, protože, stejně jako šifra lístečková, je interaktivní a vizuálně přívětivá.

Zaluštění

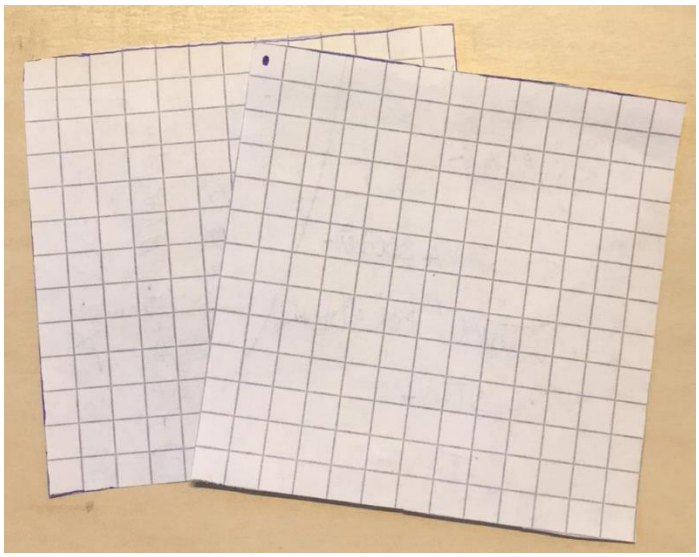
Nejprve si musíme spočítat počet znaků. Tentokrát jsme více limitovaní počtem, protože nám musí vyjít takové číslo, které je druhou mocninou nějakého čísla, tj. n^2 = [počet znaků]. Důvodem je její řešení. Mřížka musí mít čtvercový vzhled, jinak bychom si mřížkou kryli část, která vůbec není vyznačená.

V našem výchozím textu je 174 znaků, což není nejlepší. Nejbližší druhou mocninou je 169, tj. 13^2. Kdyby se nám text nepovedlo upravit na počet 169, mohli bychom použít číslo 14, protože $14^2 = 196$. Ovšem přidat 22 křížků taky není hezké, proto bychom mohli trochu upravit znění věty.

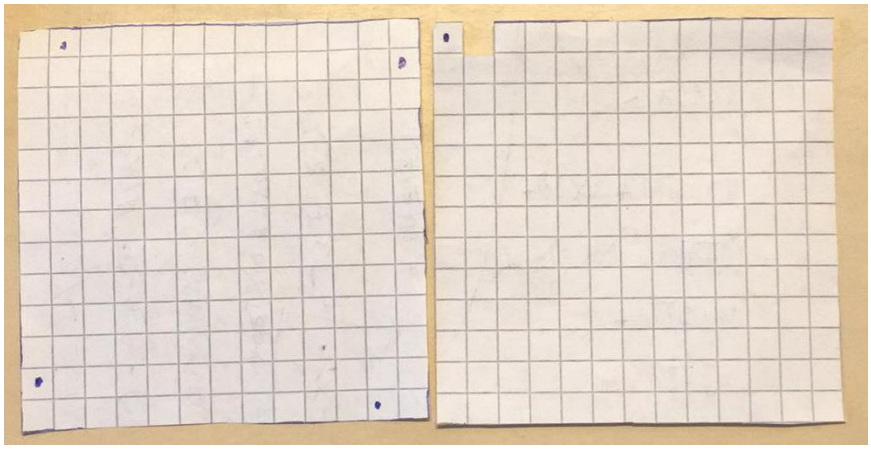
Nyní ovšem použijeme úplně novou větu se zněním „***Tato neobvyklá ryba má jako duch průsvitné tělo, takže vidíte vnitřní orgány. Při rozčílení téměř zčerná. Její jméno je Tetra fantómová.***“. Tato věta má celkově 114 znaků (pokud počítáme tečky bez čárek a písmeno CH jako jedno), ovšem během vytváření vznikla početní chyba a místo čtverce 11 × 11 vznikl čtverec 12 × 12. Tento error způsobil nadbytek křížků, což sice není veliký problém, ale nevypadá to hezky.

Neexistuje obecná mřížka, vždy jde o osobní preferenci toho, kdo zprávu zalušťuje. Pokud chce být člověk originální, může dělat složité obrazce a vyhrát si s jejím vzhledem. Proces vytváření mřížky je trochu složitý. Každý cyklus si zvolíme, který čtvereček zrovna z mřížky odstřihneme. Nejlepším způsobem je vždy odstranit čtvereček a označovat pole, která jsou po otočení vidět.

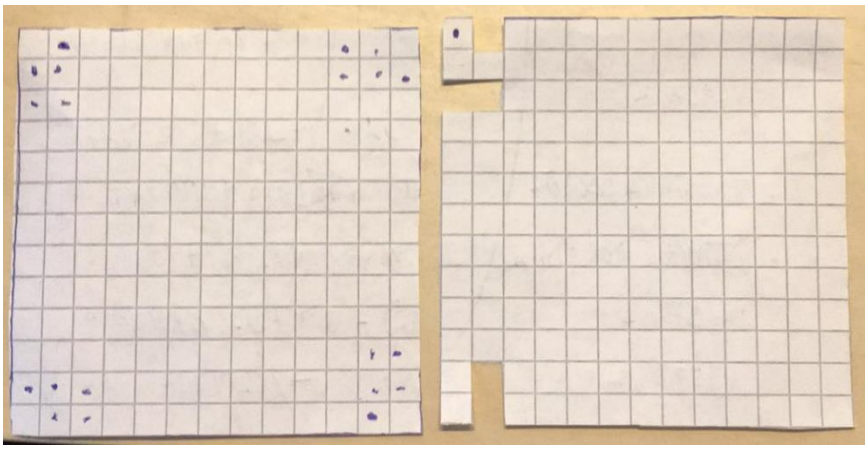
Vytváření mřížky



Obrázek 6: Připravené čtverce na mřížku



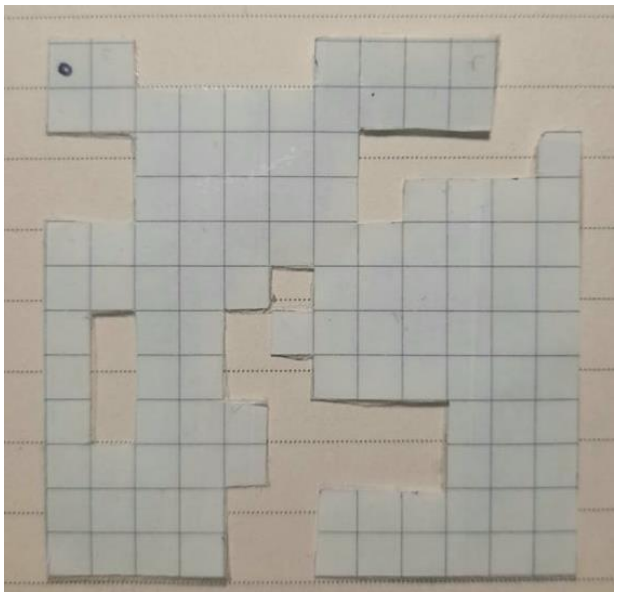
Obrázek 7: vlevo - označování bodů, vpravo – mřížka



Obrázek 8: Fáze vytváření mřížky a označování polí

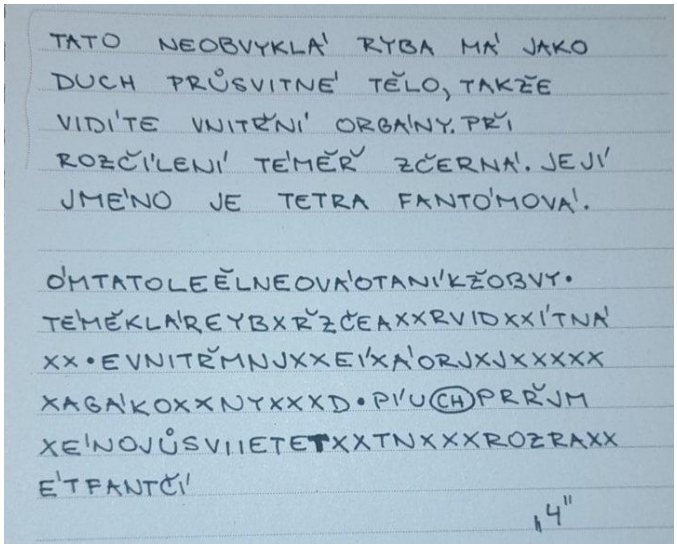
1. Vytvoříme si 2 shodné čtverce. Jedním z nich je naše mřížka, kterou označíme tečkou vlevo nahoře,
2. zvolíme si místo, které odstřihneme a učiníme tak,
3. přiložíme mřížku ke čtverci a začneme označovat místa, která jsou odhalená,

   a. začíná se tečkou vlevo nahoře,
   b. po vyznačení všech odhalených částí mřížku otočíme vpravo,
   c. proces opakujeme, dokud se nedostane tečka zpět doleva nahoru,
4. opakujeme proces 2. a 3.,
5. mřížku zabalíme do ochranné fólie (postačí izolepa) a začne se zalušťovat,
   a. do odhalených částí budeme místo teček psát náš originální text,
   b. po návratu tečky zpět doleva nahoru opíšeme text zleva doprava seshora dolu, jak stojí ve čtverci.



Obrázek 9: Hotová mřížka přiložená k textu šifry

Označuje se číslicí 4. Zároveň je k ní přiložena mřížka, kterou se šifra luští.



Obrázek 10: Původní text a zaluštěná mřížka

Vyluštění

Nejprve si musíme spočítat počet znaků a připravit si čtvereček. Následně do něj napíšeme znak po znaku zleva doprava seshora dolu. Poté nám stačí vzít mřížku a přiložit čtvereček označený tečkou do levého horního pole. Začneme opisovat veškeré znaky, které vidíme. Opisují se zleva doprava seshora

dolu. Musíme si dávat pozor, abychom žádný znak nevynechali. Až nám znaky dojdou, mřížku otočíme doprava (nyní máme tečku v pravém horním rohu) a proces opakujeme. Ve chvíli, kdy se nám tečka vrátí do levého horního rohu, šifra je vyluštěna.

Čtverec

Pátou a naší poslední táborovou šifrou je čtverec. Jedná se o relativně náročnou šifru na vyluštění, neboť když v tom nemá člověk cvik a zavedený systém, dokáže se v písmenkách snadno ztratit.

Zaluštění

Vzhledem k tomu, že opět potřebujeme načrtnout čtverec, chytře si vybereme text s počtem znaků cca 169 a opět si nakreslíme čtverec s rozměry 13 × 13. Znění nové věty ponechám tajemství a můžete sami zkusit šifru vyluštit!

Naštěstí už nemusíme nic vystřihávat a designovat, stačí nám se jen držet určité struktury. Každý znak z naší šifry přísluší určité pozici ve čtverci, která je označená číslem.

S	R	G	R	,	E	Z	J	V	É	N	R	O
O	L	V	L	C	U	H	I	T	T	M	U	U
É	L	P	T	Y	U	Ý	S	E	,	O	Y	E
J	Z	O	T	T	O	M	O	J	O	I	P	Á
K	Ý	M	V	Y	A	Č	E	D	E	Z	E	P
Í	K	R	Í	I	S	A	T	Ž	V	C	D	L
Á	N	R	T	K	.	X	D	Á	Í	C	L	A
A	U	L	L	A	P	U	O	M	V	K	N	E
V	O	T	P	L	L	T	Z	A	N	Ž	E	E
E	E	K	E	U	Ř	S	E	N	Ž	P	A	Ř
E	A	I	R	I	Ý	A	H	A	C	L	Á	O
U	E	T	K	R	,	E	R	S	Ř	D	C	E
D	V	V	Í	L	N	H	N	O	L	N	H	U

Tabulka 2: Návrh čtverce a jeho zaplnění znaky

1	5	9	13	17	21	25	29	33	37	41	45	2
48	49	53	57	61	65	69	73	77	81	85	50	6
44	88	89	93	97	101	105	109	113	117	90	54	10
40	84	120	121	125	129	133	137	141	122	94	58	14
36	80	116	144	145	149	153	157	146	126	98	62	18
32	76	112	140	160	161	165	162	150	130	102	66	22
28	72	108	136	156	168	169	166	154	134	106	70	26
24	68	104	132	152	164	167	163	158	138	110	74	30
20	64	100	128	148	159	155	151	147	142	114	78	34
16	60	96	124	143	139	135	131	127	123	118	82	38
12	56	92	119	115	111	107	103	99	95	91	86	42
8	52	87	83	79	75	71	67	63	59	55	51	46
4	47	43	39	35	31	27	23	19	15	11	7	3

Tabulka 3: Úplné zaplnění čtverce

1	5	9	13	17	21	25	29	33	37	41	45	2
48	49										50	6
44												10
40												14
36												18
32												22
28												26
24												30
20												34
16												38
12												42
8	52										51	46
4	47	43	39	35	31	27	23	19	15	11	7	3

Tabulka 4: Mezikrok čtverce, ilustrace výplně vnitřního čtverce

Až vložíme veškerá písmena do jejich příslušných polí, stačí nám text zleva doprava seshora dolu opsat. Každé číslo říká, kolikátý znak vložíme kam. Všimněte si, že se znaky píšou nejdříve do rohů a vyplní se vnější okraj čtverce. Až nám místo dojde, jednoduše se začne nový čtverec.

U čtverce je kontrola velmi důležitá.

Označuje se číslicí 5. Žádné další označení a pomocné materiály nejsou potřeba.

Vyluštění

Po vypočítání počtu znaků si připravíme čtverec, do kterého napíšeme všechny znaky zleva doprava seshora dolu. Po napsání se musíme držet stejného klíče jako při zalušťování. Nejlepší možností je si znaky vyškrtávat nejlépe tužkou, protože v případě chyby není problém gumovat. Pokud jsou na vyluštění dva, je dobré, když jeden luští a nahlas diktuje znaky, druhý opisuje text.

Závěr

Na závěr bych rád zmínil, že tento návod není jediný způsob, jak k šifrám přistupovat a jak s nimi pracovat. Je možné, že tyto šifry používáte i ve vašem oddíle a mají jiné atributy, možná máte i jiný způsob zalušťování. Proto nechci, abyste tento text brali jako definitivní. Pouze jsem se odrážel od zkušeností z našeho tábora, kde si nedokážu spoustu aktivit bez šifer ani představit. Pokud máte jiné nápady ohledně šifrování a chcete tento text použít pouze jako inspiraci, je to v pořádku. Důležité je, že vy sami dokážete těmto algoritmům porozumět a efektivně je využívat.

Doufám, že byla práce nápomocná a dokázala někomu například objasnit způsoby luštění. Pokud někdo tyto šifry vidí poprvé, neváhejte a zapojte je do chodu vašeho tábora, šifrování je zábava!

Seznam objektů